IN THE CLAIMS:
Please revise the claims, as follows:

1. (Currently amended) A method of guaranteeing authenticity of an object, said object including at least one of a chip having a first recording support and a second recording support, said method comprising:

providing a sample of material obtainable only by at least one of chemical and physical processes such that a measurable characteristic of said sample is random and not reproducible and affixing said sample to said object;

associating a ~~first~~ number reproducibly to said sample by using a specific reader;

~~forming at least one coded version of said first number, said at least one coded version being obtained by a key signature;~~ and

to allow for sample-reader combinations such that the number associated to said sample is only essentially reproducible at a time of verification, recording said ~~first~~ number on said object ~~card~~ on at least one of said first recording support ~~on one of said chip~~ and said ~~another~~ second recording support;

~~wherein said object includes at least one of a chip having a recording support positioned on said object and another recording support to permit said recording of said first number~~.

2. (Canceled)

3. (Previously presented) The method according to claim 39, wherein said object comprises a smart card.

4. (Original) The method according to claim 3, wherein said smart card incorporates a chip.

5-6. (Canceled)

7. (Currently amended) The method according to claim ~~39~~ 1, further comprising:

forming at least one coded version of said number, said at least one coded version being obtained by a key signature, wherein said key signature includes using public key cryptography; and

recording said at least one coded version on at least one of said first recording support and said second recording support.

8. (Previously presented) The method according to claim 39, further comprising:

reading, by a reader, the sample in an imprecise manner, meaning that sequential readings are not exactly the same as an initial reading of said sample, but collecting, at a time of preparation of the object, much more information about said sample that will be contained by decoding any of said coded version of that information,

wherein said object carries a chip and a recording of a digital representation of the full information initially collected of the sample from the reader used at the time the object is prepared.

9. (Original) The method according to claim 8, further comprising:

sending a result of the reader to a processor, which associates with the reading of the sample said number;

sending said number to a second processor containing a secure hash function, details of which are made public, and a secret part of said key signature, said key signature comprising a public key signature, wherein said second processor computes a coded version of the hash of said number appended with a predetermined, optional data; and

outputting said coded version to said chip.

10. (Original) The method according to claim 9, wherein upon introducing the object into a second reader, a different reading of said sample occurs such that the first reader reads the sample to deliver *R(S)* and the second reader reads the sample to deliver *R0(S0)*, said method further comprising:

determining by a comparator whether the readings by said first and second readers are less than or equal to a predetermined threshold to accept the object, at least temporarily, as authentic.

11. (Original) The method according to claim 10, further comprising:

reading said coded version by said chip and verifying said coded version against said number by using a public part of the public key signature; and

if said number and said coded version read by said chip are compatible, accepting the card as authentic.

12. (Original) The method according to claim 8, further comprising:

delivering by said reader an actual reading *R(S)* and delivering by a second reader an original reading as *R0(S0)*;

processing said readings by first and second processors to deliver *N(R(S)* and *N(R0(S0))*, respectively; and

determining by a comparator whether outputs from said first and second processors have a value no more than a predetermined threshold, to temporarily accept the object as authentic.

13. (Original) The method according to claim 12, further comprising:

reading the coded version in said chip and verifying said coded version against said number by using a public portion of a public key signature; and

if the information in said number and that read in said chip are compatible, accepting said object as authentic.

14. (Previously presented) The method according to claim 39, further comprising:

sensing a degeneration of said sample.

15. (Original) The method according to claim 14, wherein said sensing includes comparing a difference between an actual reading vector and an original reading vector against a threshold;

forwarding a result of the reader to a processor, which associates with the reading of said sample a transformed vector *K(N0(R0(S0)))*, where *K* is a transformation matrix; and

forwarding the transformed vector to a second processor including a secure hash function, details of which are made public, and a secret part of a public key signature scheme.

16. (Original) The method according to claim 15, wherein said object includes a chip, and wherein said second processor computes a coded version of the hash function of the transformed

vector appended with predetermined optional external data, to provide a coded number, said coded number being put on said chip,

wherein upon introducing the card to a second reader, a predetermined different reading of the sample is performed.

17. (Original) The method according to claim 16, wherein an actual reading made by a first reader is transformed into a transformed vector *KN*, and wherein an original transformed vector *KN0* is delivered by a second reader, and

wherein the transformed vector, *KN* is compared against the original transformed vector *KN0* by a comparator such that if the two transformed vectors have a value within a predetermined closeness, the object is temporarily accepted as authentic.

18. (Previously presented) The method according to claim 17, further comprising:

reading by said chip the coded version and verifying said coded version against the transformed vector using a public part of the public key signature; and

accepting the object as authentic if the transformed vector and the coded version read in said chip are compatible.

19. (Currently amended) The method according to claim 39, ~~wherein~~ wherein said object being authenticated comprises a piece of paper.

20. (Previously presented) The method according to claim 39, wherein a sequence of data associated with said sample, said sample, and certificates associated with said sample and said data are precomputed.

21. (Previously presented) The method according to claim 20, wherein new data and its certificate are computed dynamically.

22. (Previously presented) The method according to claim 39, wherein said key signature includes using private key cryptography.

23. (Previously presented) The method according to claim 39, wherein said specific reader captures information out of the sample by one of a scanning and globally.

24. (Previously presented) The method according to claim 39, wherein said sample includes at least one of a mineral and a glass, selectively covered by a carbon film and affixed to said object.

25. (Previously presented) The method according to claim 39, wherein said coded version of said number includes at least one of optional data appended to said number and a hash of said number with said optional data.

26. (Previously presented) The method according to claim 39, wherein data linked to the sample of material is selectively changeable.

27. (Previously presented) The method according to claim 39, wherein said sample of material is selectively changeable over time.

28. (Previously presented) The method according to claim 39, wherein said data is selectively changeable when said sample is changed.

29. (Original) The method according to claim 20, wherein said data is selectively changeable when said sample is changed.

30. (Previously presented) The method according to claim 39, wherein new data associated with said sample and a certificate of said sample are computed dynamically.

31. (Previously presented) The method according to claim 39, wherein at a time of creation of said object, said coded version of said number is stored in memory for later comparison when said object is presented for authentication.

32. (Previously presented) The method according to claim 39, wherein a plurality of coded versions of numbers are recorded into said object.

33. (Previously presented) A method of preventing cloning of an object, said method comprising:

providing a sample of material obtainable only by at least one of chemical and physical processes having a characteristic that samples obtained by said process are random and not reproducible;

associating a number reproducibly to said sample by using a specific reader as an initial measurement of said sample;

forming at least one coded version of said number by a public key signature; and

recording said number and at least one of said at least one encoded versions on said object.

34. (Currently amended) A method of preventing imitation of a smart card, said method comprising:

providing a sample of material obtainable only by at least one of chemical and physical processes having a characteristic that samples obtained by said process are random and not reproducible;

associating a number reproducibly to any said sample by using a specific reader as an initial reading of said characteristic; ~~and~~

forming at least one coded version of said number by a public key signature; and

recording said number and at least one of said at least one coded version into an area of said smart card.

35. (Previously presented) A system for guaranteeing authenticity of an object, said method comprising:

a sample of material obtainable only by at least one of chemical and physical processes having a characteristic that samples obtained by said process are random and not reproducible, said sample being placed on said object;

means for associating a number reproducibly to any said sample by using a specific reader, said specific reader providing an initial measurement of said characteristic and an initial associated number;

means for forming at least one coded version of said initial associated number, said at least one coded version being obtained by a public key signature; and

means for recording said number and said at least one coded version into an area of said object.

36. (Previously presented) A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented guaranteeing of authenticity, said method comprising:

for a sample of material obtainable only by at least one of chemical and physical processes such that the sample is random and not reproducible, associating a number reproducibly to said sample by using a specific reader;

recording said number on a recording medium on an object;

forming at least one coded version of said number; and

recording said at least one coded version of said number on said recording medium of said object.

37. (Previously presented) The method of claim 39, wherein said forming at least one coded version of said number further comprises using additional information for said forming said coded version, wherein said additional information comprises the date of issue of said object.

38. (Previously presented) The method of claim 39, wherein said forming at least one coded version of said number further comprises using additional information for said forming said coded version, wherein said additional information comprises the functionality of an application of said object.

39. (Previously presented) A method of guaranteeing authenticity of an object that includes or has attached thereto at least one of a chip with a recording support and another recording support, said method comprising:

attaching to said object a first sample of material obtainable by at least one of a chemical process and a physical process having a characteristic that samples generated by said process are random and non-reproducible, said first sample being associated with a first number obtained by reading said first sample using a first reader of a specific sort, said first number being long enough to both:

carry enough information to detect any counterfeited second sample different from said first sample but which second sample, when read with a reader of said specific sort, would generate a second reading substantially identical to said first reading of said first sample; and

contain as many digits as encryptions that are considered as safe at a time of production and expected to be safe for some years to come afterward;

recording, on at least one of said recording supports, at said time of production, in an exactly readable way, an exact value of said first number so that said first number can be checked against a later reading made with any reader of said specific sort at each time of verification of said object, thereby providing a first verification that verifies that a sample being read at said verification of said object is indeed said first sample; and

forming, at said time of production, at least one encrypted version of said first number, at least one of said encrypted versions of said first number being also recorded in an exactly readable way on said object at said time of production, said at least one encrypted version of said first number being obtained by a method from public key cryptography that is considered as safe at said time of production and expected to be safe for some years to come afterward, said recording of said at least one encrypted version thereby providing a second verification that verifies at said verification that said encrypted version of said first number was generated by an authorized party,

wherein information concerning said public key cryptography method is available so that said second verification can be made by anyone of an intended public.

40. (Previously presented) The method of claim 39, wherein said first number is encrypted in combination with further information, said further information and all encrypted versions of said first number being also recorded in an exactly readable way on said object at said time of production.

41. (Currently amended) The method of claim 39, further comprising:

forming at least one second encrypted version of said first number by a ~~non-public~~ private key cryptography encryption scheme; and

recording said at least one second encrypted version in an exactly readable manner on said object.

42. (Currently amended) A method of guaranteeing authenticity of an object that includes or has attached thereto at least one of a chip with a first recording support and ~~another~~ a second recording support, said method comprising:

attaching to said object a first sample of material obtainable by at least one of a chemical process and a physical process having a characteristic that samples generated by said process are random and non-reproducible, said first sample being associated with a first number obtained by first reading said first sample using a first reader of a specific sort to obtain a temporary first number and then extracting said first number from said temporary first number, using a statistical method, said first number being long enough to both:

carry enough information to detect any counterfeited second sample different from said first sample but which second sample, when read with a reader of said specific sort, would generate a second reading substantially identical to said first reading of said first sample; and

contain as many digits as encryptions that are considered as safe at a time of production and expected to be safe for some years to come afterward; and

forming, at said time of production, at least one encrypted version of said first number, at least one of said encrypted versions of said first number being also recorded in an exactly readable way on said object at said time of production on at least one of said first recording

support and said second recording support, said at least one encrypted version of said first number being obtained by a method from public key cryptography that is considered as safe at said time of production and expected to be safe for some years to come afterward, said recording of said at least one encrypted version thereby providing a second verification that verifies at said verification that said encrypted version of said first number was generated by an authorized party,

wherein:

information concerning said public key cryptography method is available so that said second verification can be made by anyone of an intended public, and

upon reading a sample attached to said object at a time of verification, a reader of said specific sort is to be used so that each later reading is substantially the same as an initial reading at said time of production by said first reader and a statistical method sufficiently robust to accommodate small changes in reading is to be used to produce a second number to be compared with said first number for said first verification.

43. (Currently amended) The method of claim 42, wherein said first number is encrypted in combination with further information, said further information and all encrypted versions of said first number being also recorded in an exactly readable way on said object on at least one of said first recording support and said second recording support at said time of production .

44. (Currently amended) The method of claim 42, further comprising:

forming at least one second encrypted version of said first number by a ~~non public~~ private key cryptography encryption scheme; and

recording said at least one second encrypted version in an exactly readable manner on said object on at least one of said first recording support and said second recording support.

45. (Currently amended) The method of claim 39, wherein said first number ~~comprises a number~~ is converted into and recorded in a base 3 number format.

46. (New) The method of claim 1, wherein said number is expressed as a vector vk(S), said method further comprising:

reading said number a plurality of times by said reader to determine an average Ak of said vector vk(S);

determining a small window Wk around said average Ak that defines a range of readings considered as acceptable for said sample; and

recording said average Ak and said small window Wk on at least one of said first recording support and said second recording support.

47. (New) The method of claim 1, wherein said process provides a sample that becomes unreadable after an amount of time that is predetermined, said authenticity of said object being thereby guaranteed only during a time shorter than said predetermined amount of time.

48. (New) The method of claim 1, wherein said object comprises a container having a contents therein, and said sample is attached to said container as a seal thereof, and an opening of said container causes said sample to be altered in a manner that a subsequent reading by a reader

provides a reading different from said number, thereby an authenticity of said contents is guaranteed when said subsequent reading agrees with said reading having been recorded.

49. (New) The method of claim 1, wherein said process provides a sample that degenerates over time in a manner that can be measured and said number is recorded on said object along with a time stamp when said reading occurs.

50. (New) The method of claim 49, wherein a subsequent reading of said sample is used to determine whether a negative-degeneration has occurred for said sample, thereby indicating that a tampering has occurred to said sample.

51. (New) The method of claim 1, wherein a plurality of samples S_i, $i > 1$, is attached to said object, each said sample S_i being associated with a corresponding number n_i obtained by reading said sample S_i using a reader of a specific sort; and

recording each number n_i on at least one of said first recording support and said second recording support on said object as a pair (S_i, n_i),

wherein said object is used as a payment card and a pair (S_i, n_i) is destroyed by a reader for purpose of making a unit payment.

52. (New) A method of guaranteeing authenticity of an object, said method comprising:

attaching at least one recording support to said object;

attaching to said object a first sample of material obtainable by at least one of a chemical process and a physical process having a characteristic that samples generated by said process are

random and non-reproducible, said first sample being associated with a first number obtained by a first reading of said first sample using a first reader of a specific sort, wherein said first number cannot reliably be repeated exactly during a subsequent reading by a reader of said specific sort;

extracting from said first reading an information for a second number, said second number being reliably repeatable during said subsequent reading;

encoding said second number using an encryption scheme; and

recording, on one of said at least one recording support attached to said object, said encoding of said second number.

53. (New) The method of claim 52, further comprising:

recording at least one of said first number and said second number on one of said at least one recording support attached to said object.